7A

УДК 004.9:355

О.С. Андрощук[1], А.М. Кудін[2]
[1]Національна академія Державної прикордонної служби України
імені Б. Хмельницького, м. Хмельницький
Україна, 29003, м. Хмельницький, вул. Шевченка, 46
[2]Фізико-технічний інститут , НТУУ «КПІ», м. Київ
Україна, 03056, г. Київ, пр. Перемоги, 37

Багатокритеріальна модель вибору архітектури системи нечіткого логічного висновку при аналізу ризиків безпеки інформації в хмарних обчислювальних та інших складних системах

A.S. Androschuk[1], A.M. Kudin[2]
[1]National Academy of State Border Service of Ukraine
named B. Khmelnitsky, c. Khmelnitsky
Ukraine, 29003, c. Khmelnitsky, Shevchenko st.,46
[2]Physical Technical Institute, NTUU "KPI", c. Kiev
Ukraine, 03056, c. Kiev, Pobedy ave.,37

Multicriteria Problem of Choice of Architecture for Fuzzy Inference System to Analyze the Information Security Risk in Cloud Computing and Other Complex Systems

А.С. Андрощук[1], А.М. Кудин[2]
[1]Национальная академия Государственной пограничной службы Украины
имени Б. Хмельницкого, г. Хмельницкий
Украина, 29003, г. Хмельницкий, ул. Шевченко, 46
[2]Физико-технический институт , НТУУ «КПИ», г. Киев
Украина, 03056, г. Киев, пр. Победы, 37

Многокритериальная задача выбора архитектуры системы нечеткого логического вывода для анализа рисков безопасности информации в облачных вычислительных и других сложных системах

Розглядається задача оцінки ризиків безпеки інформації в хмарних обчислювальних та в інших складних системах. Вперше запропонована модель вибору раціонального складу архітектури системи нечіткого логічного висновку (СНЛВ) для оцінки ризику в складних системах на основі розв'язання багатокритеріальної задачі. Модель надає можливість на підставі статистичних даних вибирати методи СНЛВ для різних випадків та вибрати оптимальну архітектуру СНЛВ.
Ключові слова: аналіз ризиків, багатокритеріальна оптимізація, хмарні обчислювальні системи.

The problem of risk assessment of information security in cloud computing and in other complex systems is considered. The rational choice model of architecture for fuzzy inference system (FIS) based on multicriteria decision is first proposed. The model makes possible choose FIS methods for different variants on the basis of statistical data and to choose the optimal structure for FIS.
Key words: risk assessment, multicriteria optimization, cloud computing systems.

Рассматривается задача оценки риска безопасности информации в облачных вычислительных и в других сложных системах. Впервые предложена модель выбора рационального состава архитектуры системы нечеткого логического вывода (СНЛВ) для оценки риска в сложных системах на основе решения многокритериальной задачи. Модель дает возможность на основании статистических данных выбрать методы СНЛВ для разных случаев и выбрать оптимальную структуру СНЛВ.
Ключевые слова: анализ рисков, многокритериальная оптимизация, облачные вычислительные системы.

Вступ

Вирішення завдань з оцінки ризиків пов'язано з проблемою домінування якісних, невизначених і нечітких факторів. Прикладами таких завдань може бути визначення ризиків при проектуванні комплексних систем захисту хмарних обчислювальних систем [1], оцінка ризику правоохоронними органами причетності осіб, об'єктів, транспортних засобів та вантажів до протиправної діяльності [2-4], оцінка ризику надзвичайної ситуації органами цивільного захисту, оцінка ризику військової небезпеки збройними формуваннями тощо. Серед методів урахування таких факторів значного поширення набули підходи на основі теорії нечітких множин та нечіткої логіки Л. Заде [5] із використанням системи нечіткого логічного висновку (СНЛВ). Побудова архітектури такої системи передбачає вибір низки методів та алгоритмів. Зважаючи на неоднорідність та різноманітність архітектури складних систем, які досліджувались [1-4], завдання побудови раціональної архітектури СНЛВ для кожного окремого випадку є актуальним.

Більшість підходів із вибору методів СНЛВ розглядають ситуацію прогнозу (апроксимації) функції за експериментальними даними. Емпіричним шляхом вибирають різні архітектури СНЛВ. Отримують числові прогнозні дані за певним методом, порівнюють їх із реальними даними та визначають абсолютну і відносну похибки прогнозування. За їх мінімумом визначають кращу архітектуру СНЛВ. Такий підхід не є придатним для ситуації оцінки ризиків. У цьому випадку можна оцінити побудовану СНЛВ лише під час експерименту. У роботі [6] обґрунтовується вибір того чи іншого методу одного типу із залученням емпіричних міркувань на підставі досвіду застосування, який неможливо формалізувати.

Таким чином на даний час відсутні формалізовані підходи до вибору архітектури СНЛВ взагалі та частково для завдань оцінки ризиків.

Постановка завдання. Принциповими особливостями вирішення завдання вибору раціонального варіанту архітектури СНЛВ, що визначають метод його рішення, є:

– багатокритеріальність завдання вибору;
– відсутність опису показників якості методів і кінцевого результату СНЛВ;
– різноманіття ситуацій тощо.

У зв'язку із цим вибір раціональної архітектури СНЛВ пропонується здійснити, вирішуючи класичне завдання оптимізації [7].

Мета статті – подання підходу щодо вибору раціонального складу архітектури СНЛВ із застосуванням методів багатокритеріальної оптимізації

Модель вибору раціонального складу архітектури СНЛВ

Моделі вибору раціональної архітектури СНЛВ та обґрунтування методу її дослідження представимо на прикладі вибору архітектури СНЛВ з оцінки ризиків безпеці інформації в хмарних обчислювальних системах [1] та ризику порушення законодавства з перетину державного кордону (ДК) [2-4]. Визначимо множини.

1. Множина Θ – кінцева множина об'єктів оцінки ризику $\gamma_1, \gamma_2, \dots, \gamma_n$. I – множина індексів елементів: $I=\{1,2,\dots,n\}$. Приклади об'єктів: підсистема хмарної обчислювальної

системи (віртуальні машини, які функціонують на певному хості; елементи розподіленої системи збереження інформації тощо) або особи, транспортні засоби, вантажі, що перетинають ДК.

2. Множина типів методів СНЛВ Z – кінцева множина елементів $\{z_{ki}\}$, де z_{ik} – k-й тип методів по i-му об’єкту оцінки ризику $i = \overline{1,N}$, $k = \overline{1,M}$ (наприклад, логічний висновок, імплікація, композиція, агрегування, активізація, акумуляція) (табл. 1).

3. Множина всіх методів СНЛВ W – кінцева множина елементів $\{w_{ikj}\}$, де w_{ikj} – j-й метод k-го типу по i-му об’єкту оцінки ризику (для спрощення візьмемо випадок, коли кількість методів усіх типів є однаковою) $i = \overline{1,N}$, $k = \overline{1,M}$, $j = \overline{1,L}$ (наприклад, max-min, max-prod, max-max, min-min, max-average, sum-prod, min-max) (табл. 1).

4. Множина значень характеристики (вартість, швидкість розрахунку, алгоритмічна складність прозорість (змістовна інтрепретабельність) [8]) методів – S. Елемент $s_{ikj} \in S$, $i = \overline{1,N}$, $k = \overline{1,M}$, $j = \overline{1,L}$ являє собою реалізацію характеристики w_{ikj}-го метода при аналізі ризику об’єкта $\gamma_i \in \Theta$. Потужності множин W та S збігаються:

$$|W| = |S|.$$

5. Множина вихідних значень оцінки ризику – O. Елемент $o_{ikj} \in O$, $i = \overline{1,N}$, $k = \overline{1,M}$, $j = \overline{1,L}$ характеризує реалізацію підмножини методів $\{w_{ikj}\}$ при аналізі ризику об’єкта $\gamma_i \in \Theta$.

Введемо змінну:

$$x_{ikj} = \begin{cases} 1, \text{ якщо застосувується } w_{ikj}\text{ -й метод з об’єктом } \gamma_i, \\ 0, \text{ у протилежному випадку} \end{cases} \qquad (1)$$

Відзначимо, що по кожному об’єкту оцінки ризику застосовується один метод СНЛВ (мається на увазі, наприклад, те, що одночасно два методи дефазифікації не можуть застосовуватись для оцінки ризику одного об’єкта), тобто

$$\sum_{j=1}^{L} x_{ikj} = 1. \qquad (2)$$

Основні параметри СНЛВ. Оцінка ризику об’єкта γ_i, здійснюється вибором сукупності засобів w_{ikj}, $i = \overline{1,N}$, $k = \overline{1,M}$, $j = \overline{1,L}$.

Для перевірки якості СНЛВ береться вибірка опису особи лінгвістичними змінними з кінцевими результатами.

Результатом оцінки ризику i-тої особи сукупністю (об’єднанням) методів буде вираз

$$O_i\,(\bigcup_{k=1}^{M}\bigcup_{j=1}^{L} w_{ikj}\, x_{ikj}), \qquad (3)$$

у більш загальному випадку

$$O(\bigcup_{i=1}^{N}\bigcup_{k=1}^{M}\bigcup_{j=1}^{L} w_{ikj}\, x_{ikj}). \qquad (4)$$

Цей вираз має бути мінімізовано для оцінки «повний захист від загроз» або «благонадійна особа» та максимізовано для оцінки «порушення безпеки інформації» або «порушник законодавства».

Характеристика (вартість) оцінки ризику об’єкта повинна бути мінімізована (максимізована) або, принаймні, вона не повинна перевищувати якоїсь величини, скажімо S_{oi}:

$$S_i = \sum_{k=1}^{M}\sum_{j=1}^{L} s_{ikj}\, x_{ikj} \le S_{oi}, \qquad (5)$$

де кожний доданок $s_{jki}x_{jki}$ – характеристика (вартість) реалізації $w_{jki} \in W$ метода, використаного на оцінку об’єкта $\gamma_i \in \Theta,\ 1 \le i \le N$.

Для системи в цілому це можна записати так:

$$S = \sum_{i=1}^{N} Si = \sum_{i=1}^{N}\sum_{k=1}^{M}\sum_{j=1}^{L} s_{ikj}\, x_{ikj} \le S_o, \tag{6}$$

де S_o – обмеження вартості для системи.

Тривалість оцінки ризику об’єкта повинна бути мінімізована або, принаймні, вона не повинна перевищувати граничний термін:

$$\sum_{k=1}^{M}\sum_{j=1}^{L} t_{ikj}\, x_{ikj} \le T, \tag{7}$$

де T – граничне значення часу оцінки підсистеми (вузла, віртуальної машини тощо) або особи (транспортного засобу, вантажу), яка перетинає ДК.

У прямій постановці – визначити оптимальну архітектуру СНЛВ за виразом

$$O(\bigcup_{i=1}^{N}\bigcup_{k=1}^{M}\bigcup_{j=1}^{L} w_{ikj}\, x_{ikj}) \to \max_{пор}(\min_{благ}). \tag{8}$$

При мінімумі часу середньої оцінки i-го об’єкта маємо

$$\sum_{j=1}^{L}\sum_{i=1}^{N}\sum_{k=1}^{M} t_{ik}\, x_{ik} / N \to min, \tag{9}$$

де t_{ikj} – часові витрати, необхідні для оцінки j-м методом СНЛВ k-го типу i-го об’єкта; x_{ikj} – змінна, яка дорівнює 1, якщо застосовується j-й метод СНЛВ k-го типу i-го об’єкта, і дорівнює 0 у протилежному випадку; N – кількість об’єктів; M – кількість типів методів СНЛВ; L – кількість методів СНЛВ k-го типу.

За таких обмежень:

а) на кожну СНЛВ призначається один метод k-го типу:

$$\sum_{j=1}^{L} x_{jki} = 1; \tag{10}$$

б) загальна характеристика (вартість) СНЛВ не перевищує граничну:

$$\sum_{i=1}^{N}\sum_{k=1}^{M}\sum_{j=1}^{L} s_{ikj}\, x_{ikj} \le S, \tag{11}$$

де s_{jki} – характеристика (вартість) j-го методу СНЛВ k-го типу для оцінки i-го об’єкта; S – гранична характеристика (вартість) СНЛВ.

У зворотній постановці – визначити оптимальний склад методів СНЛВ за виразом

$$O(\bigcup_{i=1}^{N}\bigcup_{k=1}^{M}\bigcup_{j=1}^{L} w_{ikj}\, x_{ikj}) \to \max_{пор}(\min_{благ}). \tag{12}$$

Загальна характеристика (вартість) забезпечення оцінки ризику об’єкта $\gamma_i \in \Theta$, $i = \overline{1,n}$ має бути мінімальною, тобто

$$\sum_{j=1}^{L}\sum_{i=1}^{N}\sum_{k=1}^{M} s_{iki}\, x_{ik} \to min. \tag{13}$$

За цих обмежень:

а) на кожну СНЛВ призначається один метод k-го типу:

$$\sum_{j=1}^{L} x_{jki} = 1; \tag{14}$$

б) середня тривалість оцінки ризику не може перевищувати граничний термін:

$$\sum_{j=1}^{L}\sum_{i=1}^{N}\sum_{k=1}^{M} t_{ik}\, x_{ik} / N \leq T, \tag{15}$$

де T – граничне значення часу оцінки підсистеми (вузла, віртуальної машини тощо) або особи (транспортного засобу, вантажу), яка перетинає ДК.

Розв'язання задач (8) – (11) та (12) – (15) надасть змогу вибрати оптимальну архітектуру СНЛВ, а вирішення відповідної сукупності завдань для всієї множини об'єктів – створити варіант інтелектуальної системи підтримки прийняття рішень.

Відомо [9], [10] , що всі численні методи розв'язання багатокритеріальних задач можна звести до трьох груп методів:

– метод головного показника;

– метод результуючого показника;

– лексикографічні методи (методи послідовних поступок).

Наявність змінної x_{ik} і характер завдання, що вирішується, вказує на необхідність застосування методів цілочисельного сепарабельного програмування для вирішення поставленого завдання [11]. Для його реалізації на відміну від цих методів авторами пропонується використання генетичного методу, який себе добре зарекомендував для вирішення завдань параметричного налаштування [12].

Перевірку адекватності розробленої моделі вибору архітектури СНЛВ здійснено за допомогою експерименту. Під час експерименту розглядались відомості, що містили значення вхідних оцінок стосовно 30 об'єктів. За результатами розрахунків найкращі результати було отримано із застосуванням методу Мамдані.

Методом активації буде *min*, який розраховується за формулою [12]:

$$\mu_{A\to B}(x, y) = \mu_A(x) \wedge \mu_A(y) = min(\mu_A(x), \mu_A(y)). \tag{16}$$

Як метод агрегування застосовується операція *min*-кон'юнкції. Для акумуляції закінчень правил вибрано *max*-диз'юнкцію. Як метод дефазифікації використовується метод центру тяжіння за формулою [12]:

$$y_0 = \frac{\int_y y\mu(y)dy}{\int_y \mu(y)dy}. \tag{17}$$

Висновки

Отже, у статті вперше подано модель вибору раціонального складу архітектури СНЛВ для оцінки ризику в складних системах на основі розв'язання багатокритеріальної задачі. Модель надає можливість на підставі статистичних даних вибирати методи СНЛВ для різних випадків. Дослідження моделі надасть змогу вибрати оптимальну архітектуру СНЛВ, а вирішення відповідної сукупності завдань для всієї множини об'єктів – створити варіант інтелектуальної системи підтримки прийняття рішень.

Литература

1. Кудін А.М. Створення систем підтримки прийняття рішень для управління захистом інформації в хмарних обчислювальних системах / А.М. Кудін // Збірник наукових праць Національної академії державної прикордонної ім. Б. Хмельницького. – 2010. – № 54. – С. 70-72.
2. Андрощук О.С. Модель нечіткого логічного виводу оцінки ризику пропуску правопорушників через державний кордон / О.С. Андрощук, Е.В. Матусяк // Збірник наукових праць ВІТІ Національного технічного університету України «КПІ». – К. : ВІТІ НТУУ «КПІ», 2011. – Випуск № 1. – С. 14-23.

3. Андрощук, О.С. Оцінка ризику щодо пропуску автотранспортних засобів у пунктах пропуску із застосуванням нечіткого логічного висновку / О. С. Андрощук, Е. В. Матусяк // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К. : ВІ КНУ, 2011. – Вип. № 33. – С. 79-86.
4. Андрощук О.С. Оцінка ризику щодо пропуску вантажів у пунктах пропуску із застосуванням нечіткого логічного висновку / О.С. Андрощук // Вісник Вінницького політехнічного інституту. – Вінниця : ВНТУ, 2011. – Вип. № 2 (95). – С. 128-133.
5. Zadeh L.A. Fuzzy Sets / L.A. Zadeh // Information and Control. – 1965. – № 8. – P. 338-353.
6. Ротштейн А.П. Интеллектуальные технологии идентификации / А.П. Ротштейн. – Винница : Универсум, 1999. – 300 с.
7. Вентцель Е.С. Исследование операций: задачи / Вентцель Е.С. – М. : Наука, 1988.
8. Штовба С.Д. Обеспечение точности и прозрачности нечеткой модели Мамдани при обучении по экспериментальным данным / С.Д. Штовба // Проблемы управления и информатики. – 2007. – № 4. – С. 102-114.
9. Кини Р.Л. Принятие решений при многих критериях предпочтения и замещения / Кини Р.Л. – М. : Радио и связь, 1981. – 342 с.
10. Дубов Ю.А. Многокритериальные модели формирования и выбора вариантов систем / Дубов Ю.А., Травкин С.И., Якимец В.Н. – М. : Наука, 1986. – 296 с.
11. Мамиконов А.Г. Достоверность, защита и резервирование информации в АСУ / А.Г. Мамиконов, В.В. Кульба. – М. : Энергоатомиздат, 1986. – 304 с.
12. Штовба С.Д. Проектирование нечетких систем средствами MatLab / Штовба С.Д. – М. : Горячая линия – Телеком, 2007. – 288 с.

Literatura

1. Kudin A.M. Zbirnyk naukovykh prats natsionalnoyi akademii derzhavnoyi sluzhby imeni B. Khmelnytskogo. 2010. № 54. S.70-72.
2. O.S.Androschuk O.S. Zbirnyk naukovykh prats VITI Natsionalnogo tekhnichnogo universitetu Ukrayiny “KPI”. K.: VITI NTUU “KPI”. 2011.Vypusk № 1. S. 14-23
3. Androschuk O.S. Zbirnyk naukovykh prats Viyskovogo institute Kiyivskogo natsionalnogo universitetu imeni Tarasa Shevchenko. K.: VI KNU. 2011. Vyp. № 33. S. 79-86.
4. Androschuk O.S. Visnyk Vinnitskogo politekhnichnogo institutu. Vyp. № 2 (95). Vinnitsa: VNTU. 2011. S. 128-133.
5. Zadeh L.A. Information and Control. 8(1965). P. 338-353.
6. Rotshtejn, A. P. Vinnica: Universum, 1999. 300 s.
7. Ventcel’ E.S. Issledovanie operacij: zadachi. M.: Nauka. 1988.
8. Shtovba S.D. Problemy upravlenija i informatiki. 2007. № 4. S. 102-114.
9. Kini R. L. Prinjatie reshenij pri mnogih kriterijah predpochtenija i zameshhenija. M : Radio i svjaz’. 1981. 342 s.
10. Dubov Ju. A. Mnogokriterial'nye modeli formirovanija i vybora variantov sistem. M.: Nauka. 1986. 296 s.
11. Mamikonov A.G. Dostovernost’, zashhita i rezervirovanie informacii v ASU. M.: Jenergoatomizdat. 1986. 304 s.
12. Shtovba, S. D. Proektirovanie nechetkih sistem sredstvami MatLab. M.: Gorjachaja linija-Telekom. 2007. 288 s.

A.S. Androschuk, A.M. Kudin

Multicriteria Problem of Choice of Architecture for Fuzzy Inference System to Analyze the Information Security Risk in Cloud Computing and Other Complex Systems

In the article, the rational choice model of architecture for fuzzy inference system (FIS) based on multicriteria decision is first proposed.

The model makes possible to choose FIS methods for different variants on the basis of statistical data. The model investigation will give opportunity to choose the optimal structure for FIS.

The solution of corresponding sets problems for the entire set of objects will give opportunity to create a variant of intellectual decision support system.

Стаття надійшла до редакції 08.06.2012.